

the authorization, approval, certification, or accreditation without change, enhancements, or upgrades.

#### § 148.12 Definitions.

*Agency.* Any "executive agency," as defined in 5 U.S.C. 105; any "Military department" as defined in 5 U.S.C. 102; and any other entity within the Executive Branch that comes into possession of classified information.

*Classified Information.* All information that requires protection under Executive Order 12958, or any of its antecedent orders, and the Atomic Energy Act of 1954, as amended.

*Cognizant Security Agency (CSA).* Those agencies that have been authorized by Executive Order 12829 to establish an industrial security program for the purpose of safeguarding classified information disclosed or released to industry.

*Cognizant Security Office (CSO).* The office or offices delegated by the head of a CSA to administer industrial security in a contractor's facility on behalf of the CSA.

*Facility.* An activity of a government agency or cleared contractor authorized by appropriate authority to conduct classified operations or to perform classified work.

*Industry.* Contractors, licensees, grantees, and certificate holders obligated by contract or other written agreement to protect classified information under the National Industrial Security Program.

*National Security.* The national defense and foreign relations of the United States.

*Senior Agency Official.* Those officials, pursuant to Executive Order 12958, designated by the agency head who are assigned the responsibility to direct and administer the agency's information security program.

#### § 148.13 Responsibilities.

(a) Each Senior Agency Official shall ensure that adequate reciprocity provisions are incorporated within his or her regulatory issuances that prescribe agency safeguards for protecting classified information.

(b) Each Senior Agency Official shall develop, implement, and oversee a pro-

gram that ensures agency personnel adhere to the policies and procedures prescribed herein and the reciprocity provisions of the National Industrial Security Program Operating Manual (NISPOM).

(c) Each Senior Agency Official must ensure that implementation encourages reporting of instances of non-compliance, without fear of reprisal, and each reported instance is aggressively acted upon.

(d) The Director, Information Security Oversight Office (ISOO), consistent with his assigned responsibilities under Executive Order 12829, serves as the central point of contact within Government to consider and take action on complaints and suggestions from industry concerning alleged violations of the reciprocity provisions of the NISPOM.

(e) The Director, Security Policy Board Staff (D/SPBS) or his/her designee, shall serve as the central point of contact within Government to receive from Federal Government employees alleged violations of the reciprocity provisions prescribed herein and the policy "Reciprocity of Use and Inspections of Facilities" of the SPB.

#### § 148.14 Procedures.

(a) Agencies that authorize, approve, certify, or accredit facilities shall provide to the SPB Staff a points of contact list to include names and telephone numbers of personnel to be contacted for verification of the status of facilities. The SPB Staff will publish a comprehensive directory of agency points of contact.

(b) After initial security authorization, approval, certification, or accreditation, subsequent reviews shall normally be conducted no more frequently than annually. Additionally, such reviews shall be aperiodic or random, and be based upon risk-management principles. Security Reviews may be conducted "for cause", to follow up on previous findings, or to accomplish close-out actions.

(c) The procedures employed to maximize interagency reciprocity shall be based primarily upon existing organizational reporting channels. These